(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 December 2000 (28.12.2000)

PCT

(10) International Publication Number
WO 00/79457 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US00/16938

(22) International Filing Date: 19 June 2000 (19.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/335,225 17 June 1999 (17.06.1999) US

(71) Applicant: INTERNET REVENUE NETWORK, INC. [US/US]; Suite #508, 3345 Wilshire Boulevard, Los Angeles, CA 90010 (US).

(72) Inventors: BENSON, David, Scott; Suite #306, 14415 Benefit Street, Sherman Oaks, CA (US). CARPENTER, Quiche', John; 7850 Fareholm Drive, Los Angeles, CA 90046 (US). JAKL, Peter; 1255 Briargate Court, Oak Park, CA 91377 (US). TROUT, Diane; Suite #112, 4851 Hazeltine Avenue, Sherman Oaks, CA 91423 (US). AHN, Chong; 2531 Chislehurst Place, Los Angeles, CA 90027 (US).

(74) Agents: SCHAAL, William, W. et al.; Blakely, Sokoloff, Taylor & Zafman, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025-1026 (US).

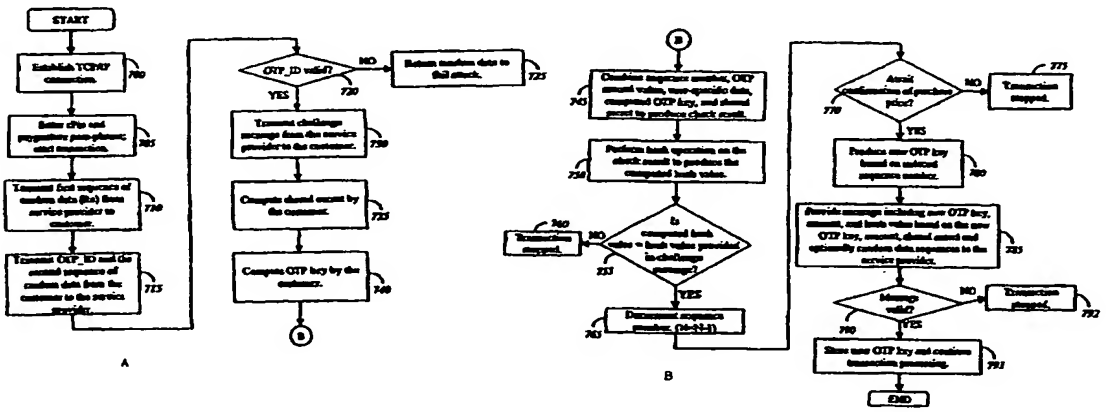
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR AUTHENTICATION OVER A PUBLIC NETWORK



(57) Abstract: A system and a method for increasing security of electronic commerce transactions over a public network. The method utilizes hash values (750) and resultant information produced from one-time pad functions (745) for authentication instead of using third party certification.

WO 00/79457 A1

SYSTEM AND METHOD FOR AUTHENTICATION OVER A PUBLIC NETWORK

1. Field

The present invention relates to the field of data security. In particular, this invention relates to a system and method for securing electronic commerce over a public network.

2. General Background

Over the last few years, personal and commercial usage of public networks has increased dramatically. One type of public network is the "Internet," an enormous compilation of publicly accessible networks situated throughout the world. Due to its growing acceptance, the Internet is quickly becoming a worldwide marketplace for products and services. For electronic commerce (e-commerce) to fully evolve, customers need access to information about the products or services being sold by a particular merchant. Also, it is important to the public at large that e-commerce implements a secure, on-line credit card payment system to avoid the perpetuation of fraud.

Recently, CyberCash, Inc. of Reston, Virginia has developed an electronic commerce payment system involving the use of an electronic wallet. An "electronic wallet" is a file stored on a hard drive of the owner of the wallet. The contents of an electronic wallet typically include sensitive information about the owner such as, for example, his or her social security number, drivers license number, credit card information (e.g., credit card number, expiration date, what financial institution issued the credit card, etc.) and the like. When purchasing a product over the Internet, the sensitive information is provided to a merchant. Thereafter, the merchant submits the credit card number and payment sum for authorization. This type of on-line electronic commerce payment system realizes a number of disadvantages.

For normal credit card payment systems, banks tend to assume a substantial amount of financial risk associated with the misuse of their issued credit cards, provided standard card verification procedures have been followed by the merchant. Normally, the card verification procedure requires the merchants to perform the following tasks: (i) verifying the identity of a credit card holder by comparing the signature on the back of the credit card with the signed charge receipt, and (ii) obtaining authorization from a payment processing system to indicate that the customer has sufficient credit before releasing the goods to the customer. Unfortunately, for e-commerce in general, a merchant cannot verify the

identity of the credit card holder because physical examination of the customer's credit card is not feasible.

If the financial risk of fraud is placed on the merchants, e-commerce will not increase in popularity because many merchants cannot assume such risk due to their limited financial resources. However, it is doubtful that banks will voluntarily assume the risk, especially when the digital content of electronic wallets is widely accessible in a plain text format. Hence, it would be desirable to develop an e-commerce authentication protocol for verifying the identity of a customer with information known only by the customer and not stored in an accessible medium.

Another general disadvantage associated with e-commerce is that electronic wallets are not portable. Rather, electronic wallets are exclusively assigned to the hard drive of the owner's computer. It would be desirable to develop a secure e-commerce network that allows a customer to conduct e-commerce transactions securely on other computers, besides his or her own computer.

Yet another disadvantage associated with conventional e-commerce authentication protocols, for each e-commerce transaction, the sensitive information is provided to a merchant. As a result, there is a greater susceptibility of fraud by merchants. It would be desirable to download sensitive information to a trusted electronic system which, in turn, would indicate to a merchant whether or not an e-commerce transaction (e.g., on-line purchase) has been authorized.

SUMMARY

Briefly, in one embodiment, the present invention relates to a method for increasing security of electronic commerce transactions over a public network between a first electronic system controlled by a customer and a second electronic system. With respect to a chosen authentication protocol, a challenge message is provided from the second electronic system to the first electronic system. The challenge message includes at least (i) a sequence number, (ii) a one-time pad (OTP) seed value, and (iii) a hash value based on the sequence number, the OTP seed value, an OTP key and a shared secret.

Upon receiving the challenge message, the first electronic system computes an OTP key and a shared secret. The OTP key based on the sequence number, the OTP seed value and a first segment of the electronic password entered by the customer. The shared secret is based on a second segment of the

entered electronic password and a segment of an electronic personal identification generated by the second electronic system and associated with the customer.

Also, the first electronic system also computes a hash value based on (i) the sequence number, (ii) the OTP seed value, (iii) the computed OTP key and (iv) the computed shared secret. This hash value is used to authenticate the second electronic system by determining that the hash value matches the hash value of the challenge message.

Other aspects and features of the invention will become apparent to those of ordinary skill in that the art upon review of the following description of embodiments of the invention in conjunction with the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is a block diagram of an illustrative embodiment of a secure e-commerce network is shown.

Figure 2 is a flowchart of an illustrative embodiment of the registration scheme to support the authentication protocol of the network of Figure 1.

Figure 3 is a flowchart of an illustrative embodiment of a registration window displayable at the customer.

Figure 4 is a block diagram of an illustrative embodiment of the operations of the OTP function during registration.

Figure 5 is a block diagram of an illustrative embodiment of the operations of the OTP functions at registration.

Figure 6 is a block diagram of an illustrative embodiment of the authentication protocol during a transaction.

Figures 7A and 7B are flowcharts of an illustrative embodiment of the authentication protocol.

Figure 8 is a block diagram of an illustrative embodiment of a purchase verification window at the customer during authentication.

DETAILED DESCRIPTION

Certain embodiments of the invention are described to provide a system and method for increasing security of electronic commerce (e-commerce) transactions over a public network. The term "secure" indicates that it is virtually infeasible for an unauthorized individual to successfully perpetuate fraud by tampering with

transmitted information without detection. Herein, examples of system architecture and protocols for registration and authentication of a customer and service provider are described. These examples should be broadly construed as illustrative in nature in order to represent the spirit of the invention.

Certain terminology is used to describe various embodiments of the system architecture. For example, an "electronic system" is broadly defined as hardware capable of processing information and accessing a public network. Each electronic system includes, but is not limited or restricted to a computer (e.g., a laptop, desktop, hand-held, server, mainframe, etc.), imaging equipment (e.g., printer, facsimile machine, etc.), a set-top box, network routing equipment and the like. The electronic systems are coupled together by a public network (e.g., a wide area network "WAN", a local area network "LAN", etc.) which has one or more communication links through which information can be routed. These communication links can be established by any type of medium such as Plain Old Telephone System (POTS) lines, cable lines, leased lines, optical fiber, electrical wire, or even wireless communication channels.

Other terminology is used to describe various aspects of the authentication protocol and the use thereof. For example, "information" includes one or more bits of data, address, control signals or any combination thereof. "Charge card information" includes one or more of the following: credit card numbers, debit card numbers, expiration date, name of the issuing financial institution, billing information concerning the credit card holder, etc. A "transaction" includes the purchase or rental of a product based on credit or an outstanding monetary balance on an account. Another examples of transactions include access requests to information stored at a web site accessible only to pre-paid members.

An "entity" includes a business, individual, partnership or other group of individuals. A "merchant" includes an entity (or hardware or software of an electronic system acting on behalf of the entity) in the business of selling goods and/or services. A "customer" includes an entity (or hardware or software of an electronic system acting on behalf of the entity) concerned with an on-line purchase from a merchant. A "service provider" includes an entity (or hardware or software of an electronic system acting on behalf of the entity) responsible for authorizing a transaction by a customer.

A. SYSTEM ARCHITECTURE (HARDWARE)

Referring now to Figure 1, an illustrative embodiment of a secure e-commerce network 100 is shown. Network 100 comprises a plurality of electronic

systems logically coupled together through a public network 110 such as the Internet for example. As shown, these electronic systems include a first electronic system (customer) 120, a second electronic system (merchant) 130 and a third electronic system (service provider) 140.

Herein, customer 120 establishes a logical connection with merchant 130 over public network 110. Normally, the logical connection is established through an Internet Service Provider (ISP) as shown by dashed lines. Customer 120 may directly access a web page produced by merchant 130 and retrieve digital advertisements therefrom. These advertisements include pictures and/or descriptions of products or services offered for sale or lease. Also, in lieu of directly accessing web pages of merchant 130, customer 120 may directly access one or more Uniform Resource Locators (URLs) associated with sponsored merchants that are displayed on a web page produced by service provider 140.

Additionally, first electronic system associated with customer 120 includes a One-Time Pad (OTP) function stored in memory. In general, during operation, the OTP function performs logical operations (e.g., exclusive OR "XOR" operations) on input information loaded into the OTP function. In particular, for this embodiment, the input information is bitwise XOR'ed with a predetermined reference, namely a sequence of bits referred to as a "OTP seed". As a result, the OTP function protects the integrity and confidentiality of input information in order to enhance security.

In this embodiment, the third electronic system associated with service provider 140 includes memory loaded with communication software (e.g., a browser), encryption/decryption software, and the OTP function. Also, service provider 140 is in communication with a remote, independent payment processing system 150 through dedicated communication links (e.g., secure leased lines) 160. Payment processing system 150 includes a database controlled by a financial institution or an agent for the financial institution responsible for authorizing debits or credits against a charge card. It is contemplated, however, that the credit/debit authorization may be performed by service provider 140 instead of being performed by a separate payment processing system 150. For example, this can be accomplished by caching invalid credit card numbers and periodically accessing payment processing system 150 for an updated listing of invalid credit card numbers.

The above-identified architecture supports a web-based, authentication protocol designed to facilitate secure on-line transactions. This authentication

protocol is a combination of "shared secret" authentication and a unique electronic transaction tag using an OTP function to validate a customer transaction. Thus, service provider 140 confirms (and perhaps determines) the approval or denial of the transaction. By securely storing all customer transaction information, service provider 140 is capable of authenticating customers and verifying transactions in order to reduce the number of "charge backs" that are common to mail order/telephone order transactions.

B. AUTHENTICATION PROTOCOL - REGISTRATION

Referring to Figure 2, a flowchart of an illustrative embodiment of a registration scheme for the authentication protocol is shown. Upon completion of the registration scheme, one or more database records for the newly registered customer are created and stored by service provider 140 of Figure 1.

As shown in block 200 of Figure 2, during registration, a customer establishes a secure logical connection (e.g., a Transmission Control Protocol/Internet Protocol "TCP/IP" connection) with the service provider of Figure 1. After establishing a secure connection, the customer prompts the service provider to transfer an applet (block 210). In one embodiment, for example, the customer selects an ActiveX-controlled object on a publicly accessible web page produced by the service provider. "ActiveX" is a library provided by Microsoft Corporation of Redmond, Washington.

Upon execution, the applet produces a sequence of events (block 220). For example, one event involves the display of a registration window 300 as shown in Figure 3. Registration window 300 includes a plurality of fields of which the contents entered into these fields are provided to the service provider. In this embodiment, the plurality of fields includes a customer information field 310, a charge field 320 and a pass-phrase field 330.

As shown in Figure 3, customer information field 310 includes billing information such as a list of name(s) and address(es) of the person or persons authorized to use the charge card(s) listed in charge field 320. Charge field 320 includes charge card information such as, for example, at least one charge card account number, the type of charge card (e.g., VISA®, Mastercard®, Discover®, American Express®, debit card from a certain financial institution, etc.), and/or the expiration date of the charge card. It is contemplated that charge field 320 may include an account routing number for a cash balance retained at a bank or by the authorization system. Pass-phrase field 330 receives, a string of alphanumeric characters (referred to as "psygnature pass-phrase") as input.

Referring back to Figure 2, a segment (e.g., a portion, rearrangement of the current content, etc.) of the psygnature pass-phrase is used for customer authentication as described in Figures 4-7. During transmission to the service provider, the billing information, credit card information and the psygnature pass-phrase are encrypted in accordance with secure socket layer (SSL) encryption protocol before transmission to the service provider (block 230). Upon receipt by the service provider, both the billing information and charge card information provided by the customer are stored into a database entry (block 240). An account number (referred to as an electronic personal identification number "ePin") is assigned to the customer and subsequently provided to the customer electronically or by mail (block 250). A segment of the ePin, referred to as an "OTP_ID," operates as an index for the database entry assigned to the customer.

While the billing information and charge card information are stored by the service provider's database, the psygnature pass-phrase is not stored anywhere in the database for enhanced security. Instead, as described below, a segment of the psygnature pass-phrase (referred to as a "OTP pass-phrase") and an OTP seed (possibly being some segment or version of the ePin) are loaded into an OTP function. In one embodiment, the OTP pass-phrase is a remainder of the psygnature pass-phrase after removal of the OTP_ID. The OTP function undergoes N iterative operations, where intermediary results are reloaded in lieu of the OTP pass-phrase to produce an OTP key, where "N" is equal to a predetermined initial sequence number (block 260). The OTP key is stored in the database entry of the service provider (block 270).

Referring now to Figure 4, a block diagram of an illustrative embodiment of the operations of the OTP function during registration is shown. To produce the OTP key, the OTP function at the service provider receives as input three sources of information, namely the OTP pass-phrase, an OTP seed and a sequence number (blocks 410 and 420). These input sources are computed from values provided by the customer (e.g., psygnature pass-phrase) or generated by the service provider (e.g., ePin). In this embodiment, the "OTP pass-phrase" is a predetermined segment of the psygnature pass-phrase that is provided by the customer during registration. The "OTP seed" is a random series of alphanumeric characters. For example, a selected series of characters associated with the ePin may be used. Of course, other variations of the ePin or data produced in a random or pseudo-random fashion may be used. In this embodiment, the series has a maximum length of 16 bits. The "sequence number" is a number that is

decremented each time there is a successful authentication. Also, the sequence number determines the number of iterations performed by the OTP function on the input sources OTP pass-phrase and OTP seed (blocks 430, 440 and 450). The final result is equal to the OTP key (block 460). Therefore, the initial starting number should be high enough to support a "maximum" number of transactions prior to a changing the OTP pass-phrase, which resets the sequence number to its default (initial) value.

Also, to reduce the likelihood of successful simulation of the service provider to trick the customer in providing confidential information, selected data is held in secret and known only by the service provider and the customer. This "shared secret" is refrained from being transmitted over the network; instead, only computations based on its value are exchanged. The shared secret is computed from predetermined segments of both the psygnature pass-phrase (provided by the customer during registration) and the ePin (generated by the service provider during registration). The shared secret is also transparently added as part of the shopper's identity at the time of registration.

For example, as shown in Figure 5, assume that the shared secret is computed by removing the 4th through 7th digits 510 of the generated 16-digit ePin (account number) 500 and the first 3 characters of every 12 characters entered by the customer for psygnature pass-phrase 520. For example, if ePin 500 is produced as "1234567890123456", the value "123890123456" (OTP_ID) 530 would be used for account identification and "4567" (SS_Pin) 510 would be available for the shared secret and, therefore, not transmitted. If psygnature pass-phrase 520 is selected by the customer to be "this is a very long password, really it is", the resultant OTP pass-phrase 540 would be "s is a velong passd" and the string "thiry wor" (SS_Pass) 550 would be used for the shared secret.

As a result, SS_Pin 510 and SS_Pass 550 are removed and combined in accordance with a selected combination (e.g., concatenation, modulo addition, etc.) 560 to produce shared secret 570. The remainder of ePin 500 and psygnature pass-phrase 520, namely OTP_ID 530 and OTP pass-phrase 540 are used for addressing and production of the OTP key, respectively.

Additionally, as an option, the customer may be prompted to select an image from a list of images stored at the service provider. Upon selection of an image by the customer, during each transaction, the image is transferred to the customer for display on a purchase verification window. This prohibits Trojan horse attacks.

C. AUTHENTICATION PROTOCOL - TRANSACTIONS

Referring now to Figures 6, 7A and 7B, a block diagram and flowcharts of an embodiment of the authentication protocol followed during a transaction are shown. The authentication protocol is initially performed over a TCP/IP connection established between customer 120 and service provider 140. Prior to these operations, customer 120 has followed the registration scheme as described above. Also, customer 120 has selected different goods and/or services to purchase through the use of a well-known shopping cart application and has selected a payment object supplied by the merchant's web page. This establishes the TCP/IP connection with service provider 140 (block 700).

Once the TCP/IP connection is established, customer 120 enters his or her ePin and the psygnature pass-phrase into an appropriate field of a purchasing window and selects an A-OK button (block 705). As an option, both customer 120 and service provider 140 exchange sequences of random information 600 and 605 in order to reduce the threat of attack. In particular, service provider 140 internally generates and transmits a first sequence of random data (Ra) 600 to customer 120 (block 710). Customer 120 responds by sending OTP_ID 610 along with a second sequence of random data (Rb) 605 generated by customer 120 (block 715). OTP_ID 610 operates as an index to access a database entry associated with customer 120.

Thereafter, service provider 140 begins authentication of customer 120 by first detecting if OPT_ID 610 is invalid (block 720). This can be accomplished by searching through a number of list of indices associated with a look-up table for example. If OTP_ID 610 is invalid, random data is returned to customer 120 so that additional resources are required of an attacker (block 725). If OTP_ID 610 is valid, service provider 140 transmits a challenge message 615 back to customer 120 as shown in Figure 6 (block 730). "Challenge message" 615 contains a current sequence number (N) 620 stored in the database entry, an OTP seed value (OSV) 625 (perhaps a segment of the ePin used in the initial computation of the OTP key), customer specific data (UD) 630 such as an assigned image selected by the customer during registration, for example, and a hash value 635. Hash value 635 is the result produced by a hash function on a combination of sequence number (N) 620, OTP seed value (OSV) 625, customer specific data (UD) 630, a current OTP key computed by service provider 140 (OK) 640, shared secret (SS) 645 and optionally first and second random data sequences (Ra and Rb) 600 and 605.

Upon receiving challenge message 615, customer 120 computes a shared secret 650 based on a hash value of selected segments (SS_Pass, SS_Pin) of customer entered psygnature pass-phrase 655 and ePin 660 (block 735). Also, an OTP key 665 is computed based on contents (OTP pass-phrase) of the customer entered psygnature pass-phrase 655, sequence number 620 and OTP seed value 625 (block 740). Customer 120 combines the provided sequence number (N) 620, OTP seed value (OSV) 625, customer specific data (UD) 630 with computed OTP key 665 and shared secret 660 to produce a check result 670 (block 745). Check result 670 undergoes a hash operation to compute a hash value 675, which is compared to hash value 635 (blocks 750 and 755). If hash values 635 and 675 do not match, the transaction ceases because the data has been modified and/or service provider 140 is not authenticated (block 760).

If hash values 635 and 675 compare, the current sequence number 620 is decremented (N-1) as shown in block 765. Also, the following items are displayed on a purchase verification window as shown in Figure 8. For example, the total purchase amount is displayed in a first field 800 while an image is displayed in a second field 810. The customer can visually check that the image is represented in second field 810 matches the registered image. If the image is different, the customer knows not to proceed with the transaction.

Referring back to Figures 6 and 7, in the event that the image is identical to the registered image and the total purchase amount is correct, the customer selects an A-OK button 820 (see Figure 8) as shown in blocks 770 and 775. Initially, this prompts the OTP function at customer 120 to produce a new OTP key (NOK) 680 based on N-1 iterations of OTP pass-phrase 661 and OTP seed value 625 (block 780). A message including new OTP key 680 and purchase amount (AMT) 685 is provided to service provider 140. Additionally, a hash value 690 featuring new OTP key 680, AMT 685, shared secret 665 and optionally random data sequences 600 and 605 is produced to verify that the sequence number and OTP seed have not been tampered with and that service provider 140 knows the shared secret information (block 785).

The message is validated by applying one extra iteration of the OTP function on new OTP key 680 to produce result 695. Result 695 is compared with the stored (current) OTP key 640 (block 790). If result 695 matches stored OTP key 640, the shopper can continue (block 791). Otherwise, service provider 140 ceases the transaction and sends a "Failure" message and customer 120 responds accordingly (block 792).

If the newly computed OTP key 680 matches OTP key 640 stored in the database, the database is updated with this new OTP key 680 and decrements the sequence number for the next transaction. Customer 120 and service provider 140 will now receive different keys for the next authentication. The sequence number is decremented so hackers cannot compute sequences given historical data.

The entire communications between customer and service provider are protected by secure socket (SSL) encryption/decryption.

While certain exemplary embodiments have been described and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not restrictive on the broad invention, and that this invention not be limited to the specific constructions and arrangements shown and described, since various other modifications may occur to those ordinarily skilled in the art. Rather, the invention should be construed from the following claims.

CLAIMS

What is claimed is:

1. A registration method for increasing security of electronic commerce over a public network, the registration method comprising:

receiving charge card information and an electronic password in an encrypted format by a first electronic system coupled to the public network;

decrypting the charge card information for storage on the first electronic system;

decrypting the electronic password;

producing a one-time pad (OTP) key; and

storing the OTP key for customer authentication of subsequent transactions along with the charge card information.

2. The registration method of claim 1, wherein the decrypting of the charge card information provides at least one of a charge card number for a charge card belonging a customer, and billing information of the customer including a name and a billing address of the customer.

3. The registration method of claim 1, wherein the producing of the OTP key comprises:

selecting a first segment of the electronic password;

producing a sequence number;

producing a one-time pad (OTP) seed value;

generating the OTP key based on the first segment of the electronic password, the sequence number and the OTP seed value.

4. The registration method of claim 3 further comprising:

generating an electronic personal identification number for a customer.

5. The registration method of claim 4 further comprising:

selecting a first segment of the electronic personal identification number;

selecting a second segment of the electronic password;

performing a hash operation on a combination of the first segment of the electronic personal identification number and the second segment of the electronic

password to produce a secret shared between the first electronic system and a second electronic system controlled by the customer.

6. The registration method of claim 5 further comprising:

returning the electronic personal identification number to the second electronic system, a second segment of the personal identification number being used to access a database entry containing the charge card information and the OTP key.

7. The registration method of claim 6 further comprising:

performing a hash operation on a combination of the first segment of the electronic personal identification number provided by the first electronic system and the second segment of the electronic password entered by the customer to produce the secret shared between the first and second electronic systems.

8. A method for increasing security of an electronic commerce transaction over a public network between a first electronic system controlled by a customer and a second electronic system, comprising:

providing a challenge message from the second electronic system to the first electronic system, the challenge message including (i) a sequence number, (ii) a one-time pad (OTP) seed value, and (iii) a hash value based on the sequence number, the OTP seed value, an OTP key and a shared secret;

computing an OTP key at the first electronic system based on the sequence number, the OTP seed value and a first segment of an electronic password entered at the first electronic system;

computing a shared secret based on a second segment of the entered electronic password and a segment of an electronic personal identification associated with the customer; and

authenticating the second electronic system by (i) computing a hash value based on the sequence number, the OTP seed value, the computed OTP key and the computed shared secret, and (ii) comparing the hash value to the hash value of the challenge message.

9. The method of claim 8, wherein the challenge message including customer specific information including an image previously selected by the

customer for verifying that the challenge message originated from the second electronic system.

10. The method of claim 8, wherein the hash value of the challenge message is based on the customer specific information.

11. The method of claim 8, wherein prior to providing the challenge message, the method comprises:

transferring a first sequence of random data from the second electronic system to the first electronic system; and

transferring a second sequence of random data and information to address a database entry containing the sequence number, the OTP seed value, the OTP key, and the shared secret associated with the customer.

12. The method of claim 11, wherein the hash value of the challenge message is further based on the first sequence of random data and the second sequence of random data.

13. The method of claim 8 further comprising:

decrementing the sequence number if the hash value matches the hash value of the challenge message.

14. The method of claim 13 further comprising:

computing a new OTP key based on the first segment of the entered password, the decremented sequence number and the OTP seed value.

15. The method of claim 14 further comprising:

generating a message by the first electronic system, the message including the new OTP key, an amount of the electronic commerce transaction, and a hash value based on the new OTP key, the amount and the shared secret; and

providing the message to the second electronic system.

16. The method of claim 15 further comprising:

providing the OTP seed value to a one-time pad (OTP) function; and

performing the OTP function on the new OTP key for an additional iteration to produce a result;

comparing the result with the OTP key; and

allowing the electronic commerce transaction to proceed if the result matches the OTP key.

17. The method of claim 8, wherein the OTP key is produced by performing an OTP function based on inputs including the first segment of the electronic password, the OTP seed value and the sequence number.

18. The method of claim 8, wherein the shared secret is produced by performing an hash function based on inputs including a second segment of the electronic password and a segment of an electronic personal identification number generated by the second electronic system and assigned to the customer.

19. A medium having embodied thereon a data packet processed by an electronic system to perform an on-line purchase of goods or services, the data packet comprising:

a header routine includes an Internet Protocol address of the electronic system; and

a payload including a new one-time pad (OTP) key computed reiteratively one less cycle than an OTP key currently stored in the electronic system, an amount of the transaction and a hash value based on the new OTP key, the amount and a shared secret known only by the electronic system and the source of the data packet.

20. The medium of claim 19, wherein the hash value of the payload further includes a plurality of sequences of random data exchanged between the electronic system and the source of the data packet.

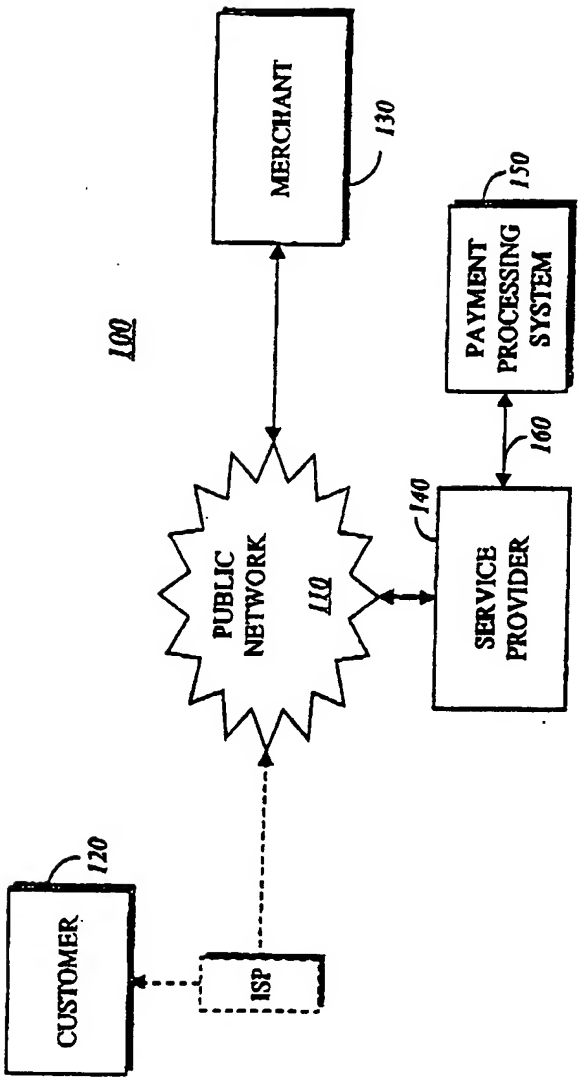


Figure 1

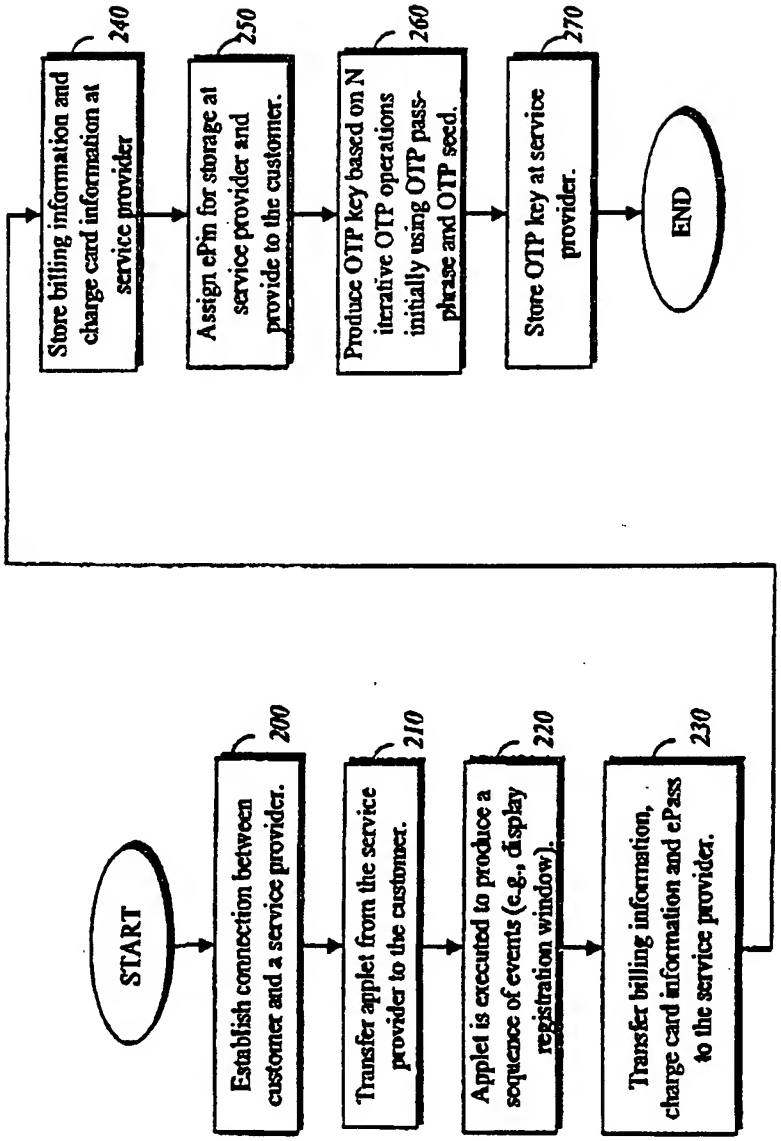


Figure 2

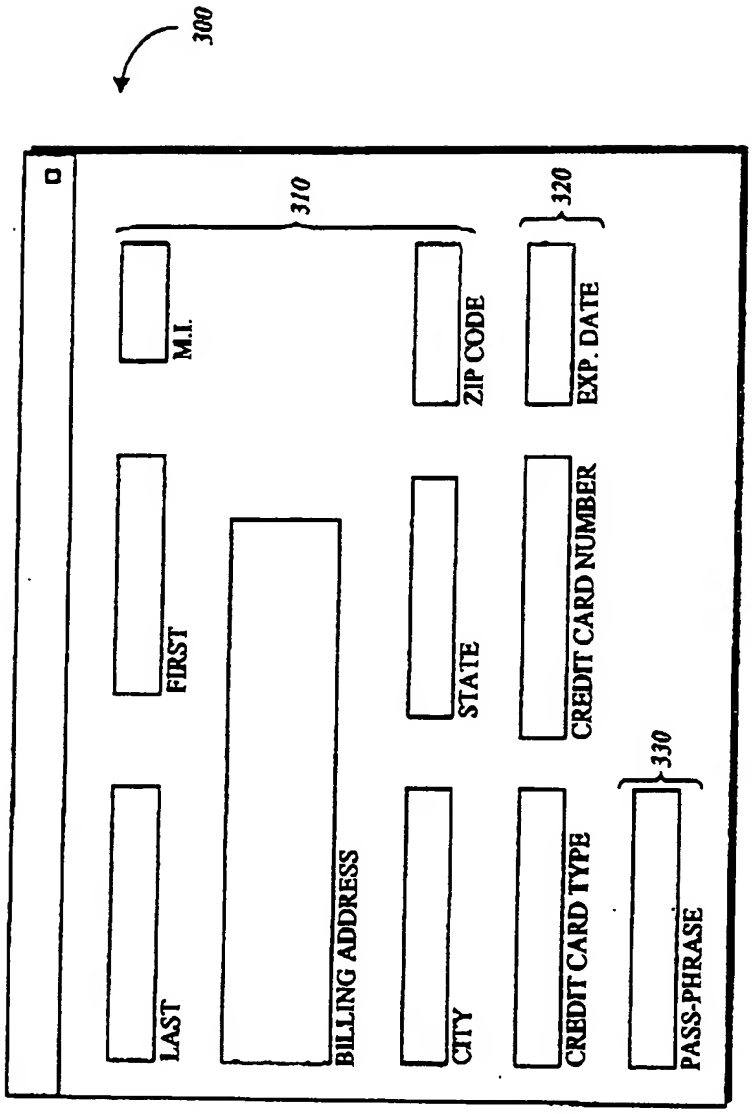
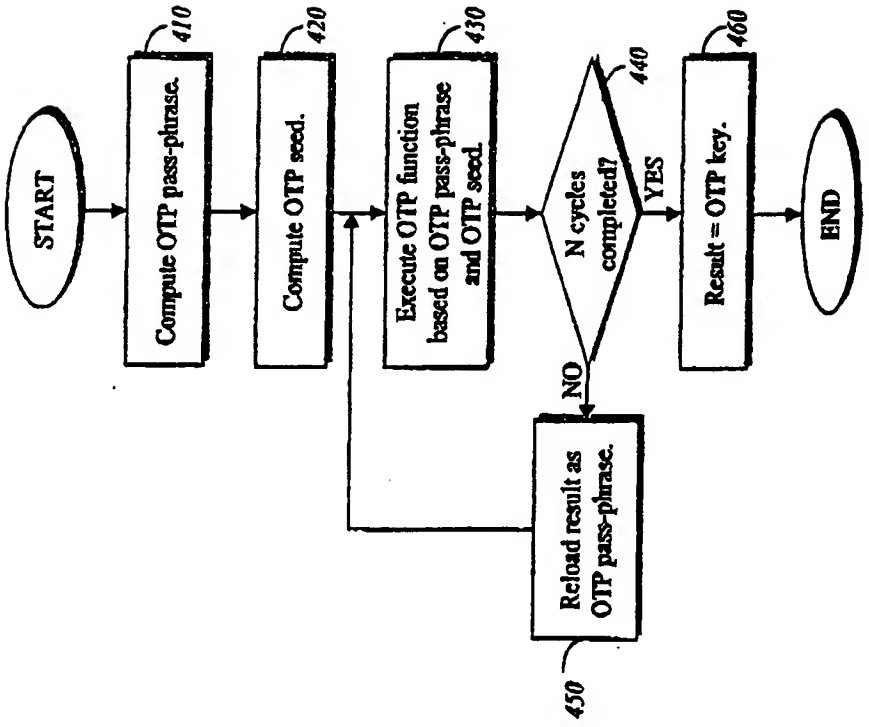


Figure 3

Figure 4


START
Compute OTP pass-phrase.
410
Compute OTP seed.
420
Execute OTP function based on OTP pass-phrase and OTP seed.
430
N cycles completed?
440
YES
NO
Result = OTP key.
460
END
Reload result as OTP pass-phrase.
450

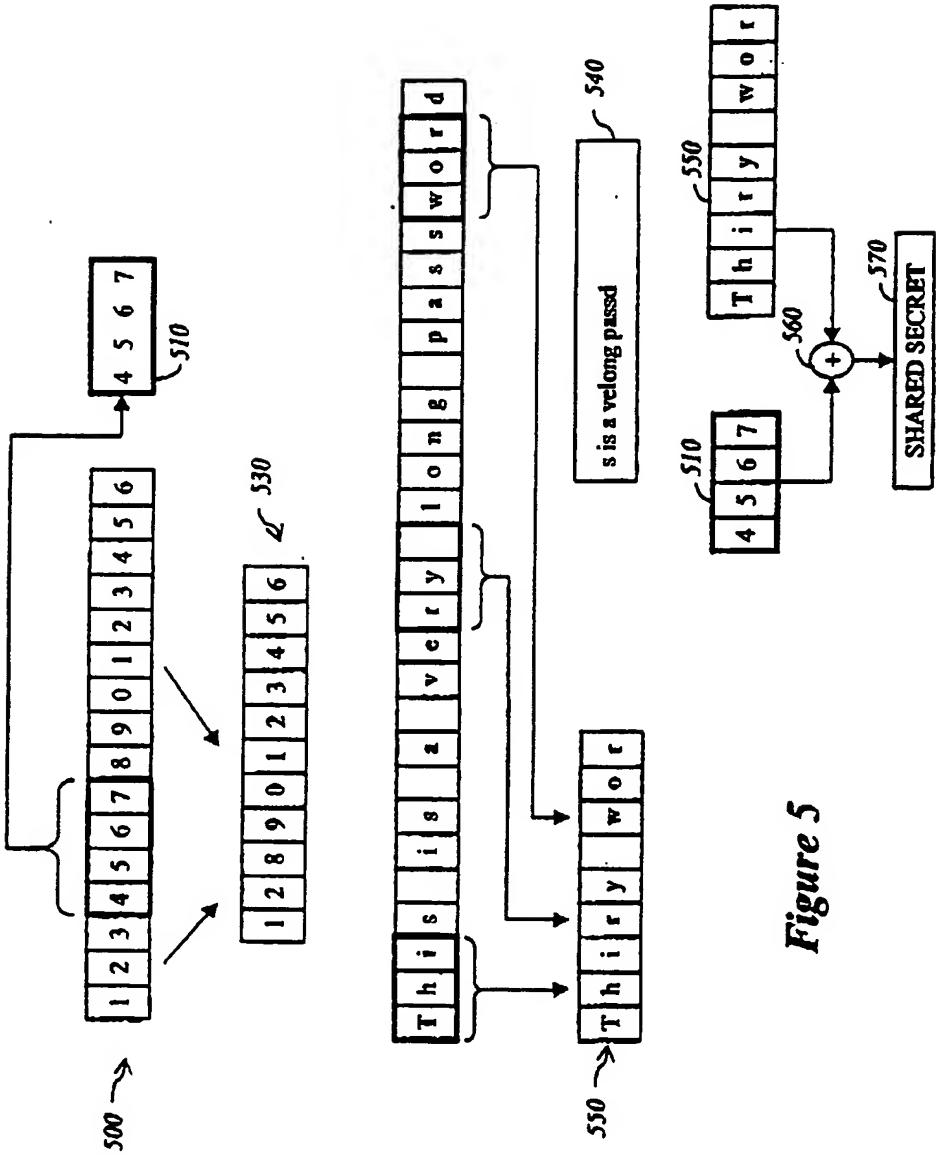


Figure 5

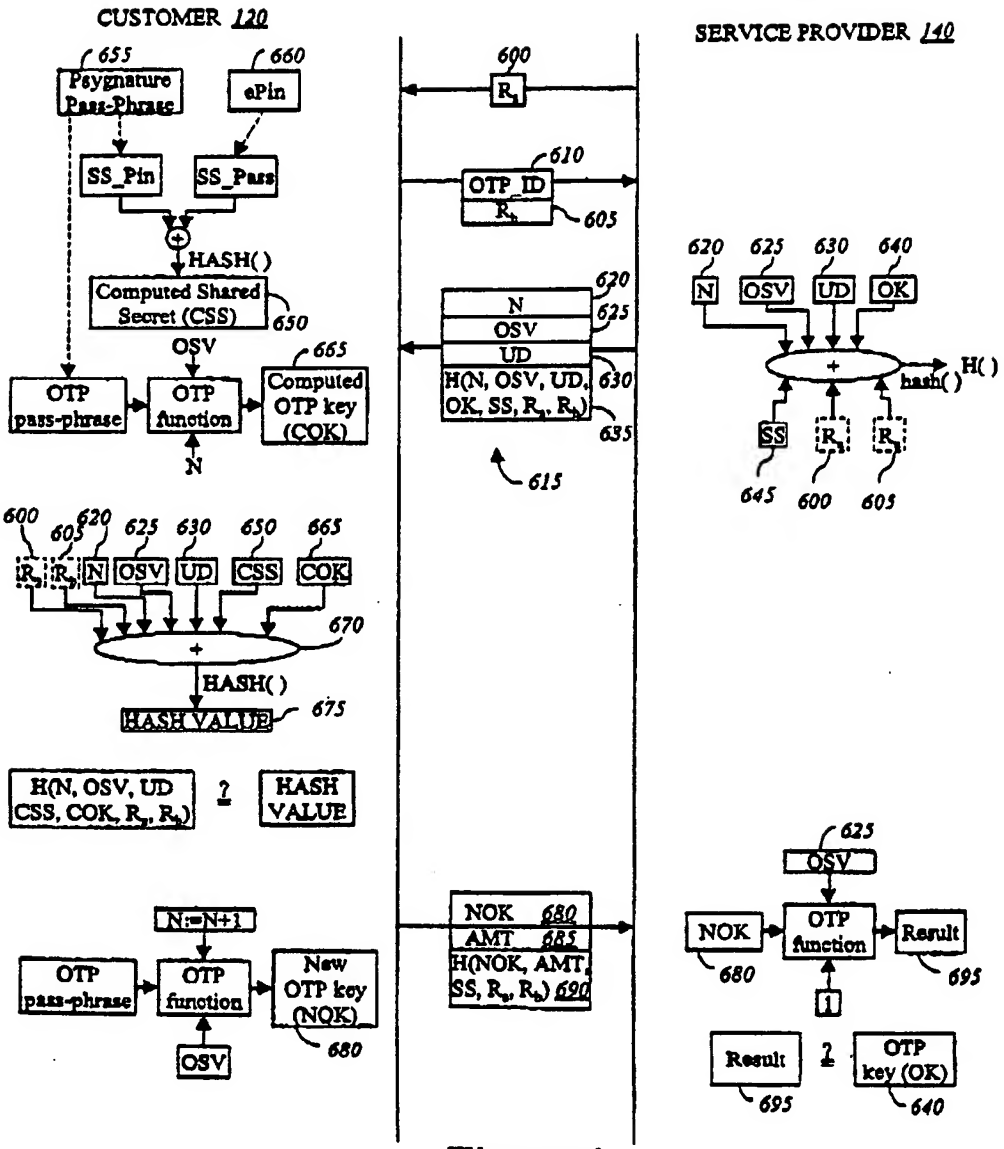


Figure 6

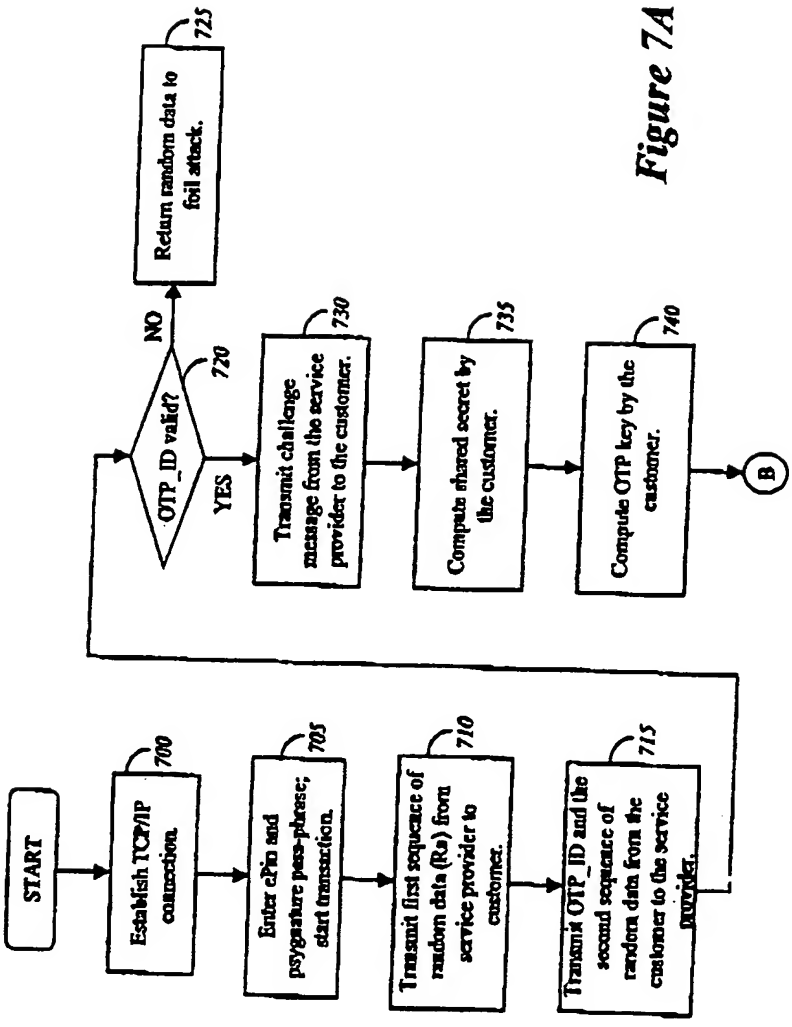


Figure 7A

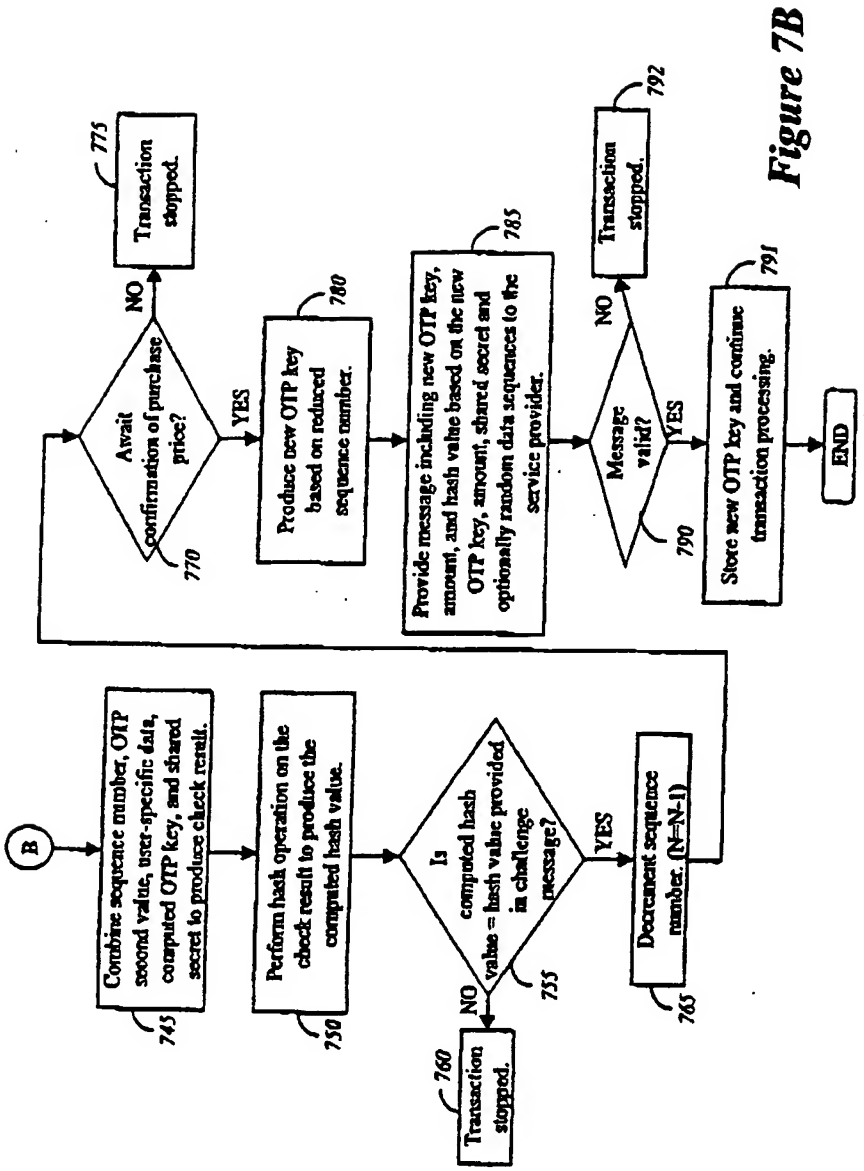


Figure 7B

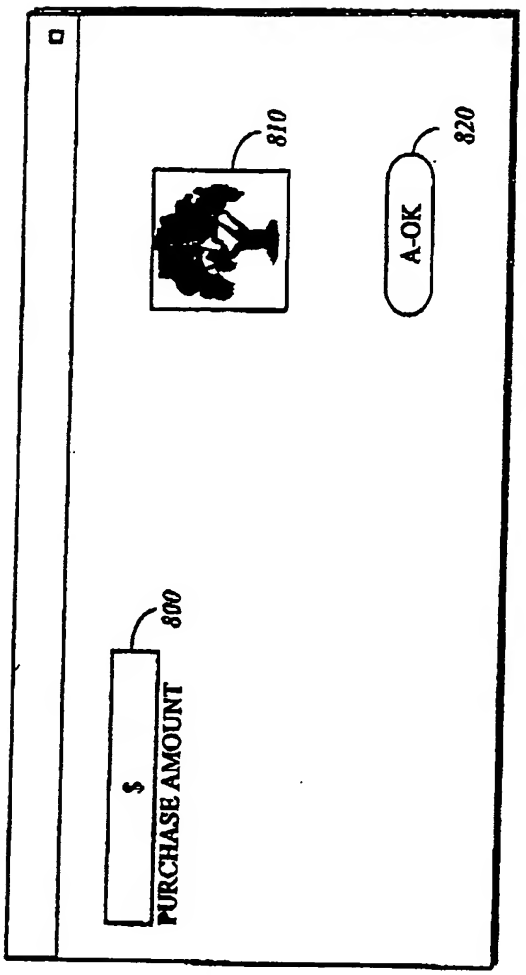


Figure 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/16938

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 17/60
US CL :705/44

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/44, 39, 41, 42, 43

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Please See Extra Sheet.

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,903,882 A (ASAY ET AL.) 11 May 1999, the background and the summary of the invention, col.1 lines 11-25, col.17 lines 28-42, col.41 lines 32-33.	1-20
Y	US 5,889,863 A (WEBER) 30 March 1999, the abstract, the background and the summary of the invention, col.16 lines 10-30, col.61 line 49 to col.62 line 4, col. 119 lines 30-41, col.120 lines 6-17,	1-20
Y	US 5,819,092 A (FERGUSON ET AL.) 06 October 1998, the background and the summary of the invention, col.28 lines 43-51.	1-20

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 18 AUGUST 2000	Date of mailing of the international search report 05 SEP 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer CUONG H. NGUYEN James R Matthews Telephone No. (703) 305-4553

Form PCT/ISA/210 (second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/16938

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,796,834 A (WHITNEY ET AL.) 18 August 1998, the background of the invention, col.3 lines 30-50, col.7 lines 32-47, col.9 lines 1-10, col.9 line 42 to col.10 line 10, col.14 lines 33-49, col.15 lines 43-54, col.18 lines 4-17, col.22 lines 17-30,	1-20
A,E	US 6,088,456 A (MCCRACKEN ET AL.) 11 July 2000, the background of the invention, col.1 lines 3-9, col.7 lines 41-67, col.8 lines 35-56.	1-20
Y	US 5,862,260 A (RHOADS) 19 January 1999, the background of the invention, col.42 lines 37-50, col.57 lines 1-27, col.48 lines 26-61, col.58 lines 5-31, col.59 lines 8-15, col.61 lines 42-51, col.66 lines 26-51, col.74 lines 36-67.	1-20
A	US 5,502,766 A (BOEBERT ET AL) 26 March 1996, the background and the summary of the invention.	1-20
Y	US 5,499,297 A (BOEBERT) 12 March 1996, the background of the invention, col.26 lines 13-29.	1-20
A	US 5,276,735 A (BOEBERT ET AL.) 04 January 1994, the background and the summary of the invention.	1-20
Y	US 5,272,754 A (BOERBERT) 21 December 1993, the background of the invention, col.2, lines 59-63, col.3 lines 47-64, col.4 lines 3-13, 28-35 and 48-63, col.5 lines 1-11, col.5 line 40 to col.6 line 4, col.7 lines 3-24, col.8 lines 3-13, col.11 lines 29-36.	1-20

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/16938

B. FIELDS SEARCHED
Documentation other than minimum documentation that are included in the fields searched:

Microsoft Press, Computer Dictionary 3rd edition.
Considine, Van Nostrand's Scientific Encyclopedia, 6th edition.
Downes et al., Barron's Dictionary of Finance and Investment Terms, 5th edition.

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

WEST2.0/DERWENT, DIALOG CLASSIC, NPL (PROQUEST DIRECT & CORPORATE RESEARCH NET), WWW (WITH NETSCAPE)
search terms: registration, charge card, information, network, password, decrytion, encryption, one-time pad key, authentication, segment, select, generate, produce, hash operation, identification, combination, message, access, database, hash value, challege message, data packet, Internet Protocol, address